CLAIMS

We claim:

1. A method of blocking attacks on a protected computer network, comprising:
receiving a plurality of packets from a network, each said packet having a packet time to live (TTL) value and belonging to a corresponding packet flow;
storing the smallest packet TTL value received from each said corresponding packet flow; and
prior to transmitting each said packet, setting said packet TTL value to said smallest packet TTL value received for said corresponding packet flow.

2. The method of Claim 1, wherein said storing the smallest packet TTL value comprises:
associating and epoch with said stored smallest packet TTL value; and
if said epoch is greater than a predefined value, discarding said stored smallest packet TTL value.

3. The method of Claim 1, further comprising periodically resetting said stored smallest packet TTL value to a maximum value.

4. The method of Claim 1, wherein said setting said packet TTL value comprises:
determining if said corresponding packet flow is on an unrestricted list; and
if said corresponding packet flow is on said unrestricted list, setting said packet TTL value to a maximum value.

5. The method of Claim 1, wherein said setting said packet TTL value comprises:
determining if said corresponding packet flow is on an unrestricted list; and
if said corresponding packet flow is on said unrestricted list, leaving said packet TTL value unchanged.

6. An apparatus for blocking attacks on a protected computer network, comprising:

means for receiving a plurality of packets from a network, each said packet having a packet time to live (TTL) value and belonging to a corresponding packet flow;

means for storing the smallest packet TTL value received from each said corresponding packet flow; and

means for setting said packet TTL value to said smallest packet TTL value received for said corresponding packet flow prior to transmitting each said packet.

7. The apparatus of Claim 6, wherein said means for storing the smallest packet TTL value comprises:

means for associating and epoch with said stored smallest packet TTL value; and

means for discarding said stored smallest packet TTL value if said epoch is greater than a predefined value.

8. The apparatus of Claim 6, further comprising means for periodically resetting said stored smallest packet TTL value to a maximum value.

9. The apparatus of Claim 6, wherein said means for setting said packet TTL value comprises:

means for determining if said corresponding packet flow is on an unrestricted list; and

means for setting said packet TTL value to a maximum value if said corresponding packet flow is on said unrestricted list.

10. The apparatus of Claim 6, wherein said means for setting said packet TTL value comprises:

means for determining if said corresponding packet flow is on an unrestricted list; and

means for leaving said packet TTL value unchanged if said corresponding packet flow is on said unrestricted list.

11. An apparatus for blocking attacks on a protected computer network, comprising:

a packet classifier configured to receive a plurality of packets from a network, each said packet having a packet time to live (TTL) value and belonging to a corresponding packet flow;

a memory configured to store the smallest packet TTL value received from each said corresponding packet flow; and

a TTL rewrite unit configured to set said packet TTL value to said smallest packet TTL value received for said corresponding packet flow prior to transmitting each said packet.

12. The apparatus of Claim 11, wherein said memory comprises:

first control means for associating and epoch with said stored smallest packet TTL value; and

second control means for discarding said stored smallest packet TTL value if said epoch is greater than a predefined value.

13. The apparatus of Claim 11, further comprising control means for periodically resetting said stored smallest packet TTL value to a maximum value.

14. The apparatus of Claim 11, wherein said TTL rewrite unit comprises:

first control means for determining if said corresponding packet flow is on an unrestricted list; and

second control means for setting said packet TTL value to a maximum value if said corresponding packet flow is on said unrestricted list.

15. The apparatus of Claim 11, wherein said TTL rewrite unit comprises:

first control means for determining if said corresponding packet flow is on an unrestricted list; and

second control means for leaving said packet TTL value unchanged if said corresponding packet flow is on said unrestricted list.

16. A computer system for use in blocking attacks on a protected computer network, comprising computer instructions for:

receiving a plurality of packets from a network, each said packet having a packet time to live (TTL) value and belonging to a corresponding packet flow;

storing the smallest packet TTL value received from each said corresponding packet flow; and

prior to transmitting each said packet, setting said packet TTL value to said smallest packet TTL value received for said corresponding packet flow.

17. The computer system of Claim 16, wherein said computer instructions for storing the smallest packet TTL value comprise computer instructions for:

associating and epoch with said stored smallest packet TTL value; and

if said epoch is greater than a predefined value, discarding said stored smallest packet TTL value.

18. The computer system of Claim 16, further comprising computer instructions for periodically resetting said stored smallest packet TTL value to a maximum value.

19. The computer system of Claim 16, wherein said computer instructions for setting said packet TTL value comprise computer instructions for:

determining if said corresponding packet flow is on an unrestricted list; and

if said corresponding packet flow is on said unrestricted list, setting said packet TTL value to a maximum value.

20. The computer system of Claim 16, wherein said computer instructions for setting said packet TTL value comprise computer instructions for:

determining if said corresponding packet flow is on an unrestricted list; and

if said corresponding packet flow is on said unrestricted list, leaving said packet TTL value unchanged.

21. A computer-readable medium storing a computer program executable by a plurality of server computers, the computer program comprising computer instructions for:

receiving a plurality of packets from a network, each said packet having a packet time to live (TTL) value and belonging to a corresponding packet flow;

storing the smallest packet TTL value received from each said corresponding packet flow; and

prior to transmitting each said packet, setting said packet TTL value to said smallest packet TTL value received for said corresponding packet flow.

22. The computer-readable medium of Claim 21, wherein said computer instructions for storing the smallest packet TTL value comprise computer instructions for:

associating and epoch with said stored smallest packet TTL value; and

if said epoch is greater than a predefined value, discarding said stored smallest packet TTL value.

23. The computer-readable medium of Claim 21, further comprising computer instructions for periodically resetting said stored smallest packet TTL value to a maximum value.

24. The computer-readable medium of Claim 21, wherein said computer instructions for setting said packet TTL value comprise computer instructions for:

determining if said corresponding packet flow is on an unrestricted list; and

if said corresponding packet flow is on said unrestricted list, setting said packet TTL value to a maximum value.

25. The computer-readable medium of Claim 21, wherein said computer instructions for setting said packet TTL value comprise computer instructions for:

determining if said corresponding packet flow is on an unrestricted list; and

if said corresponding packet flow is on said unrestricted list, leaving said packet TTL value unchanged.

26. A computer data signal embodied in a carrier wave, comprising computer instructions for:

receiving a plurality of packets from a network, each said packet having a packet time to live (TTL) value and belonging to a corresponding packet flow;

storing the smallest packet TTL value received from each said corresponding packet flow; and

prior to transmitting each said packet, setting said packet TTL value to said smallest packet TTL value received for said corresponding packet flow.

27. The computer data signal of Claim 26, wherein said computer instructions for storing the smallest packet TTL value comprises computer instructions for:

associating and epoch with said stored smallest packet TTL value; and

if said epoch is greater than a predefined value, discarding said stored smallest packet TTL value.

28. The computer data signal of Claim 26, further comprising computer instructions for periodically resetting said stored smallest packet TTL value to a maximum value.

29. The computer data signal of Claim 26, wherein said computer instructions for setting said packet TTL value comprise computer instructions for:

determining if said corresponding packet flow is on an unrestricted list; and

if said corresponding packet flow is on said unrestricted list, setting said packet TTL value to a maximum value.

30. The computer data signal of Claim 26, wherein said computer instructions for setting said packet TTL value comprise computer instructions for:

determining if said corresponding packet flow is on an unrestricted list; and

if said corresponding packet flow is on said unrestricted list, leaving said packet TTL value unchanged.